

WHAT IS CLAIMED:

- Sub
a1
1. A method for dynamically configuring a tunnel comprising:
initiating, by a first peer, a negotiation with a second peer;
sending, by the second peer, information to the first peer;
extracting, by the first peer, a security configuration from the information sent by the
second peer; and
establishing, using the security configuration, a tunnel between the first peer and the
second peer.
 2. The method of claim 1, wherein the negotiation utilizes the configuration mode
exchange extension of the IPSec protocol.
 3. The method of claim 1, wherein the establishing a tunnel includes conducting a
phase2 negotiation in the IPSec protocol.
 4. The method of claim 1, further comprising initiating, by the first peer, a
preliminary negotiation with the second peer.
 5. The method of claim 4, wherein the initiating a preliminary negotiation includes
conducting a phase1 negotiation in the IPSec protocol.
 6. A method for dynamically configuring a tunnel comprising:
initiating, by a first peer, a negotiation with a second peer;

extracting, by the first peer, a security configuration from information sent by the second peer; and

establishing, using the security configuration, a tunnel between the first peer and the second peer.

7. The method of claim 6, wherein the tunnel is an IPSec tunnel.

8. The method of claim 6, wherein the negotiation utilizes the configuration mode exchange extension of the IPSec protocol.

9. The method of claim 6, wherein the initiating comprises requesting, by the first peer, that the second peer send information, the information including policy information to define a subsequent negotiation between the first peer and the second peer.

10. The method of claim 9, wherein the policy information defines one or more security associations.

11. The method of claim 10, wherein the information sent by the second peer comprises sets of attributes, the attributes including security parameters and network addresses.

12. The method of claim 6, wherein the establishing a tunnel comprises negotiating, by the first peer with the second peer, to generate a secure key.

20. The method of claim 17, wherein the initiating a preliminary negotiation further comprises sending, by the first peer to the second peer, the identity of the first peer.

21. The method of claim 17, wherein the initiating a preliminary negotiation includes conducting a phase 1 negotiation in the IPSec protocol.

22. The method of claim 17, wherein the preliminary negotiation utilizes one of main mode and aggressive mode of the IPSec protocol.

23. A method for dynamically configuring a tunnel comprising:
sending, by a second peer, information to a first peer that initiated a negotiation with the second peer, the information including a security configuration intended to be extracted by the first peer; and
establishing, using the security configuration, a tunnel between the first peer and the second peer.

24. The method of claim 23, wherein the information includes policy information defining one or more security associations.

25. A system for dynamically configuring a tunnel comprising:
a first peer; and
a second peer configured to communicate with the first peer over a network connection,
wherein the first peer is configured to initiate a negotiation with the second peer,
the second peer is configured to send information to the first peer,

the first peer is configured to extract a security configuration from the information sent by the second peer, and

the first peer and the second peer are configured to establish a tunnel therebetween using the security-configuration.

26. The system of claim 25, wherein the tunnel is an IPSec tunnel.

27. A computer-readable medium encoded with a plurality of processor-executable instruction sequences for:

initiating, by a first peer, a negotiation with a second peer;

extracting, by the first peer, a security configuration from information sent by the second peer; and

establishing, using the security configuration, a tunnel between the first peer and the second peer.

28. The computer-readable medium of claim 27, wherein the negotiation comprises a request/reply negotiation, wherein the first peer requests that the second peer send the information, and the second peer replies to the request by sending the information to the first peer.

29. A computer-readable medium encoded with a plurality of processor-executable instruction sequences for:

sending, by a second peer, information to a first peer that initiated a negotiation with the second peer, the information including a security configuration intended to be extracted by the first peer; and

30. The computer-readable medium of claim 29; wherein the information includes sets of attributes, the attributes including security parameters and network addresses.

[illegible]